Risico's in de netwerksamenleving

Koops, E.J.; van der Hof, S.; Bekkers, V.J.J.M.

Published in:
ICT en openbaar bestuur

Publication date:
2005

B.J. Koops, S. van der Hof & V. Bekkers (2005), 'Risico's in de netwerksamenleving: over vervlochten netwerken en kwetsbare overheden', in: Lips, Bekkers & Zuurmond (red.), *ICT en openbaar bestuur*, Utrecht: Lemma 2005, p. 671-706.

Risico's in de netwerksamenleving: over vervlochten netwerken en kwetsbare overheden

Bert-Jaap Koops, Simone van der Hof & Victor Bekkers[1]

Aanleiding

De samenleving van de 21ste eeuw wordt ook wel de netwerksamenleving genoemd (Castells, 1996). In de netwerksamenleving zijn sociaal-organisatorische netwerken, ICT-netwerken en allerlei fysieke netwerken en infrastructuren onlosmakelijk met elkaar verbonden. Moderne informatie- en communicatietechnologie is doorgaans een noodzakelijke voorwaarde voor het goed laten functioneren van tal van netwerken en infrastructuren. Denk daarbij aan de rol die ICT speelt in de distributie van gas, water en electriciteit, het vervoer van mensen over het spoor, over de weg, door de lucht en over het water, maar ook de rol die ICT speelt in de uitwisseling van informatie, kennis en in de communicatie tussen organisaties en mensen. Amsterdam-Zuidoost als economische locatie en als economisch knooppunt – met een hoge mate van zakelijke en ICT-gerichte dienstverlening – leunt voor de veelvoud van activiteiten die daar worden verricht, op ICT-netwerken. Hetzelfde geldt ook voor de haven van Rotterdam als sociaal-organisatorisch netwerk. Het gevolg is dat een verstoring in het ene netwerk gevolgen heeft voor het functioneren van het andere netwerk. Menig treinreiziger kan hierover meepraten. Een sein- of wisselstoring door falende computers op het baanvlak Gouda-Utrecht leidt niet alleen tot een verstoring van het verkeer op dit traject, maar korte tijd later spreiden de effecten zich uit tot andere baanvlakken over het gehele land. Kortom, de netwerksamenleving is een kwetsbare samenleving en deze kwetsbaarheid geldt ook voor de overheid. Zij maakt immers deel uit van diezelfde netwerksamenleving en is ook grotendeels afhankelijk van de wisselwerking tussen verschillende netwerken en infrastructuren (uitgebreid Bekkers e.a., 2002). Bovendien heeft zij als taak de integriteit en stabilitieit van deze netwerken te garanderen.

Er zijn veel voorbeelden te geven die laten zien, hoe diep ICT is doorgedrongen in de haarvaten van het openbaar bestuur, en hoe kwetsbaar de informatiehuishouding van overheidsorganisaties is, te meer daar talrijke bedrijven en burgers hiervoor afhankelijk zijn.

Zo schreef in 1995 de rechtbank Den Haag een aantal computers af. Een studente uit Nijmegen kocht er één, en trof op de harde schijf diverse verslagen van forensische psychiaters en van politieverhoren aan, en ook correspondentie van rechters, officieren van justitie en griffiers. Zij stuurde een en ander door naar een regionale krant.[2] De Divisie CRI in Den Haag installeerde een nieuw computersysteem; kort daarna werden verdachten op vrije voeten gesteld en onschuldigen gearresteerd. Het computersysteem werd buiten werking gesteld – helaas was het reservesysteem inmiddels ook ontmanteld. Volgens de leverancier had de politie het systeem onjuist gebruikt (Neumann, 1995:175-6). In Rotterdam wist een ambtenaar voor zo'n 6 miljoen gulden te verduisteren door telkens na de geautomatiseerde controle betaalopdrachten toe te voegen aan het gemeentelijke betaalsysteem.[3]

Een officier van justitie nam eens zo'n 50 diskettes met justitiële informatie mee naar huis, die bij een inbraak werden ontvreemd. De informatie werd doorgegeven aan de pers, waarmee de officier – en justitie – in grote verlegenheid werd gebracht (Enquêtecommissie, 1996:187).

---

[1] Bert-Jaap Koops en Simone van der Hof zijn uhd respectievelijk senior-onderzoeker ICT-recht bij het Centrum voor Recht, Bestuur en Informatisering van de Universiteit van Tilburg. Victor Bekkers is hoogleraar bestuurskunde aan de Erasmus Universiteit Rotterdam. Zij danken Roger Jolly voor zijn hulp bij dit artikel.

[2] Persbericht ANP 8 december 1995.

[3] HR 15 januari 1991, NJ 1991, 668 m.nt. C.

Dieven ontvreemdden in december 1996 een schootcomputer van de KLPD in Zeist; de draagtas bleek een briefje te bevatten met de toegangscode tot de computer.[4] Mitterand stopte op zijn eerste dag als president het papiertje met de code om een kernwapen te lanceren in zijn jasje, waarna hij er niet meer aan dacht. Het papiertje werd nog juist onderschept voordat het pak de stomerij inging.[5] Hackers uit Nederland achterhaalden honderden militaire geheimen van de VS tijdens de eerste Golfoorlog; dit had misschien het verloop van de oorlog kunnen veranderen, als Saddam Hussein ten minste de hackers geloofd zou hebben.[6] Begin jaren 1990 waarde een virus door China dat de computergebruiker vroeg of hij de toenmalige premier Li Peng een goede premier vond; wie ja antwoordde, zag vervolgens zijn harde schijf gewist (Kristof & WuDunn, 1994:279).
Het Nederlandse reserve-communicatiesysteem voor hulpverleners werd ooit getest tijdens een rampoefening. Toen het publieke telecommunicatienet uitviel, bleek het reservenet niet te werken. Ook werd veel geïnvesteerd in een volledig zelfstandig operationeel netwerk voor overheid en hulpverleners, C2000; de (reeds later dan aangekondigde) gedeeltelijke invoering hiervan bleek de nodige onvolkomenheden te vertonen: in een ziekenhuis mocht bijvoorbeeld niet mobiel worden gebeld vanwege het stralingsgevaar dat kritische apparatuur zou kunnen verstoren; diverse gebruikers vielen bij de oefening terug op het oude systeem. Het draagvlak van het nieuwe systeem laat te wensen over.[7]

Dit is een vrij willekeurige opsomming voorbeelden die aangeven wat er mis kan gaan met de informatiehuishouding van de overheid. Vanzelfsprekend geeft dit een vertekend beeld: veel, erg veel gaat goed, en vermoedelijk zijn bovenstaande voorbeelden grotendeels incidenten. Toch leren dergelijke voorbeelden twee dingen. In de eerste plaats blijkt er een grote diversiteit te bestaan aan wat er mis kan gaan: de kwetsbaarheid heeft vele kanten. Ten tweede suggereren diverse voorbeelden dat de gevolgen van een beveiligingsincident groot kunnen zijn, soms zelfs rampzalig. Dat betekent dat ook als de kans op een incident klein is, het risico niettemin groot kan zijn: het risico wordt immers gevormd door de kans vermenigvuldigd met de mogelijke schade. De kwetsbaarheid bestaat dus niet alleen uit de menigvuldige bronnen van beveiligingslekken, maar ook uit de potentiële gevolgen ervan.

Dit hoofdstuk geeft een overzicht van deze door ICT-netwerken geëntameerde kwetsbaarheid van het openbaar bestuur die noodzakelijkerwijs deel uitmaakt van de netwerksamenleving. Die kwetsbaarheden worden zichtbaar zowel op het niveau van de samenleving als op het niveau van een individuele overheidsorganisatie. In paragraaf twee en drie gaan we in op enkele oorzaken en verschijningsvormen hiervan. Daarbij pendelen we tussen meer macro-sociologische concepten rond het ontstaan van risico's (voortbouwende op het werk van Castells, Beck en Douglas & Wildavsky) en tussen de organisatorische manifestatie van deze risico's, waarbij we ons vooral richten op kwetsbaarheden in de informatiehuishouding van de overheid. We spreken in dit verband over ICT-kwetsbaarheid. In paragraaf vier gaan we in op een aantal organisatorische bronnen van ICT-kwetsbaarheid. In paragraaf 5 geven we aan hoe de Nederlandse overheid in beleidsmatige zin op deze kwetsbaarheid heeft gereageerd. De beleidsagenda wordt geschetst. Vervolgens worden in paragraaf zes mogelijke maatregelen besproken om deze kwetsbaarheid tegen te gaan. Daarbij maken we een onderscheid tussen primair technische en primair organisatorische maatregelen. We bespreken daarbij ook de juridische context van deze maatregelen. Tot slot gaan wij in op de rol die de overheid en private partijen spelen in een kwetsbare netwerksamenleving: hoe kan informatiebeveiliging van de maatschappij het beste worden bevorderd?

[4] *Kamerstukken II* 1996/97, 25 208, nr. 1.
[5] *De Volkskrant* 18 mei 1995.
[6] Tim Reid, 'Hackers pillaged US files to sell secrets to Saddam', *Electronic Telegraph* 23 maart 1997.
[7] Zie het kritische rapport van de Algemene Rekenkamer uit juni 2003, *Kamerstukken II* 2002/03, 28 970, nrs. 1-2, te vinden op <http://www.c2000.nl/contents/pages/00018821/rapport_rekenkamer.pdf>.

2. Oorzaken

Wat zijn de voornaamste oorzaken van ICT-kwetsbaarheid?

Technologische vernieuwing
Een eerste belangrijke oorzaak is de voortdurende vernieuwing van ICT en de nog steeds toenemende complexiteit van computers. Waar de systemen complexer worden, ontstaan ook meer potentiële gaten, simpelweg omdat ook de ontwerpers het geheel niet meer overzien.

Interconnectiviteit en penetratie
Een tweede oorzaak is de toenemende interconnectiviteit en de penetratie van ICT-netwerken in het alledaagse functioneren van mensen en organisaties. ICT is doorgedrongen tot in de haarvaten van uiteenlopende menselijke activiteiten: "that is by their penetration of all domains of human activity, not as an exogeneous source of impact, but as a fabric in which such activity is woven" (Castells, 1996:31). ICT is een onderdeel geworden van het DNA van tal van maatschappelijke processen. Waar vroeger nog veelal analoge en off-line alternatieven beschikbaar bleven als de techniek de organisatie in de steek liet, zijn er momenteel steeds minder alternatieven voorhanden. Áls er dan iets gebeurt, bijvoorbeeld als de stroom twee uur lang uitvalt, het netwerk een dag platligt, of een harde schijf verongelukt, zijn de gevolgen en daarmee de schade meteen veel groter dan voorheen. "Burgers, bedrijven en de overheid zijn feitelijk zo gewend geraakt aan onze zo goed lopende maatschappij en zo afhankelijk geworden van allerhande vormen van voorzieningen, dat een kleine kink in de kabel al snel grote gevolgen heeft door de mate van afhankelijkheid die wij ons vaak niet genoeg realiseren."[8]
De vervlechting van deze netwerken leidt ertoe dat er wereldwijde, nieuwe organisatie- en productievormen ontstaan die een 'informationele ruimte' vormen en die processen van globalisering (van het ecomomische, sociale en culturele leven) ondersteunen. Castells (1996:412) spreekt in dit verband over 'a space of flows' die wordt omschreven als "the material organization of timesharing social practices that work through flows". Vrij vertaald bedoelt hij hiermee een dusdanige organisatie van stromen (zoals kapitaal, beelden, geluiden, symbolen, teksten en interacties tussen mensen en organisaties) in de vorm van een netwerk, waardoor het mogelijk is om sociaal handelen in de tijd op elkaar af te stemmen zodat tijd geen enkele belemmering meer oproept voor effectief sociaal handelen. Dit elektronische netwerk zorgt ervoor dat bepaalde plaatsen en knooppunten ('hubs' en 'nodes') met uiteenlopende sociale, culturele, economische, fysieke, politieke en andere functionele eigenschappen met elkaar worden verbonden (Castells, 1996:413). Wall Street is zo'n knooppunt van kapitaalstromen in de wereld. Het zijn vooral deze knooppunten die kwetsbaar zijn voor allerlei aanvallen van buitenaf (zoals terroristische aanslagen) maar ook door aanvallen van binnenuit (zoals fraude).

Integratie
Ten derde, en hiermee samenhangende, zien we dat de penetratie van ICT in onze alledaagse werkelijkheid, vooral gepaard gaat met een toenemende convergentie van allerlei specifieke technologieën naar hoogwaardig geïntegreerde systemen die, mede vanwege hun complexiteit, ook weer kwetsbaar zijn (Castells, 1996:61-63). De belangrijkste hefboom om dit technologisch integratieproces te bewerkstelligen is een ontwikkeling die digitalisering heet (Negroponte, 1995). De digitalisering van beeld, geluid, tekst en andere vormen van informatie en kennis betekent dat deze informatie wordt omgezet in een uniforme en binaire code (dit wil zeggen in nullen en enen). Hierdoor wordt het mogelijk om deze beelden, geluiden, teksten etc. naar hartelust te integreren, te manipuleren en te verzenden. Dit betekent niet alleen dat verschillende technische toepassingen zoals televisie, pc, video, cd-rom, fax en (mobiele) telefonie aan elkaar kunnen worden gekoppeld maar ook de daarbij behorende infrastructuren. Maar dit is nog slechts het begin. We zien namelijk dat hieraan nieuwe technieken zoal satelliettechnologie en allerlei

[8] *Kamerstukken II* 2002/03, 26 643, nr. 39, p. 2.

biometrische technieken zoals DNA-profilering en irisscans aan worden toegevoegd. De metafoor van de digitale snelweg verwijst in dit verband naar het combineren en op elkaar aansluiten van allerlei soorten van infrastructuren en technologietoepassingen, waardoor een interactieve, flexibele en op individuele wensen en behoeften toegesneden uitwisseling en integratie van woord, geluid, beeld en biometrische informatie mogelijk wordt (Bekkers & Huigen, 1994). In de ogen van Negroponte betekent het proces van digitalisering een kwalitatieve breuk met de industriële samenleving, die primair in het teken stond van de verplaatsing van atomen en moleculen (grondstoffen zoals kolen en ijzer, gas, water, halffabrikaten zoals staal en elektriciteit, en eindproducten zoals auto's en koelkasten) en daarvoor speciaal aangelegde vervoersinfrastructuren. Digitalisering zorgt voor een de-materialisering van het maatschappelijk en economische verkeer. Dit heeft vooral gevolgen voor de transporteerbaarheid en manipuleerbaarheid van kennis en informatie, hetgeen op zichzelf weer nieuwe kwetsbaarheden oproept.

Open netwerken
Ten vierde zien we dat organisaties meer en meer gebruikmaken van open netwerken als het Internet en daarmee blootstaan aan bedreigingen uit vele hoeken. Het Internet is inherent onveilig, want de structuur is juist dusdanig ingericht dat het netwerk als geheel blijft functioneren ook als vele onderdelen ervan zijn platgelegd. Tegen 'kleine' aanvallen op individuele knooppunten en computers die aan het netwerk hangen, is geen primaire beveiligingsstructuur geschapen. De kwetsbaarheid van grootschalige onderling verbonden netwerken wordt versterkt door de enorme gebruikersgroep: van overal over de wereld kunnen krakers één bepaalde computer aanvallen.

Hackerscultuur
Hiermee samen hangt een vijfde oorzaak: de hackerscultuur, waarbinnen het als sport wordt gezien om computers binnen te dringen. Deze is inmiddels niet meer zo sterk als in de begintijd van het Internet (vergelijk daarover Himanen, 2001), maar nog altijd bestaat er een subcultuur van technojongeren die over de hele wereld gaten in beveiligingssystemen opsporen, liefst van prominente overheidsorganisaties. Hoewel dit vaak gebeurt met goede bedoelingen (namelijk om de beheerder te waarschuwen dat zijn systeem onveilig is), zijn er twee aspecten die de kwetsbaarheid vergroten: er kan onbedoeld grote schade worden aangericht doordat een computerkraker niet precies weet wat hij doet wanneer hij is binnengedrongen, en het vertrouwen in de integriteit van het systeem en de informatie wordt onherstelbaar beschadigd bij een inval, ook al beweert de indringer dat hij niets anders dan een waarschuwing op het scherm van de systeembeheerder heeft achtergelaten.

Sluitpost
Een andere oorzaak is dat de beveiliging van computersystemen vaak een sluitpost is. Beveiliging kost immers veel en moet voortdurend worden geactualiseerd, maar het levert geen zichtbare voordelen op. Integendeel: een goed beveiligd systeem kent geen beveiligingsincidenten, zodat de eigenaar zich zal kunnen afvragen waarom het nu zo nodig was om die beveiliging aan te schaffen. Slechts als er daadwerkelijk iets mis gaat, wordt meestal gegrepen naar beveiligingsmaatregelen. Soms – als de schrik er flink in zit – gebeurt dat op een goede manier, door een integraal beveiligingsbeleid op te stellen; vaak echter blijft het bij lapwerk en wordt alleen datgene beveiligd wat er in concreto fout ging. De deur blijft dan open staan voor talloze andere incidenten.

Geheimhouding
Een zevende oorzaak is het mechanisme van de fluistercultuur rond beveiligingsincidenten. Een organisatie die slachtoffer is van een beveiligingsincident probeert dit meestal geheim te houden en zo spoedig mogelijk intern af te handelen, uit angst voor imagoschade. Het gevolg hiervan is

echter dat zwaktes in computersystemen en netwerken niet snel publiekelijk bekend worden gemaakt zodat andere organisaties zich hiertegen kunnen wapenen. De aangiftebereidheid bij computeraanvallen blijft nog steeds laag, waardoor een systematische aanpak van computercriminaliteit bepaald niet wordt bevorderd.[9] Ook bevordert dit niet een cultuur van leren, over de grenzen van organisaties heen.

We hebben in deze paragraaf een aantal oorzaken aangegeven waarom de netwerksamenleving een kwetsbare samenleving is. Gewezen is onder meer op de toenemende afhankelijkheid van ICT in het alledaagse functioneren van organisaties. Maar hoe staat het met de effecten die optreden? Hoe moeten we die waarderen?

3. De risicosamenleving

De toenemende afhankelijkheid van ICT is een verschijningsvorm van de hedendaagse risicosamenleving. De notie van risicosamenleving, of 'risk society' zoals die onder meer wordt beschreven door Beck (1999), is in dit verband interessant, omdat het a) inzicht geeft in het ontstaan van risico's en b) inzicht geeft in de effecten van risico's.
Rampen, calamiteiten en andere gevaren zijn zo oud als Methusalem en maken onlosmakelijk deel uit van elke vorm van samenleven. Brand,oorlog, hongersnood, overstromingen zijn van alle tijden en alle plaatsen. Het proces van modernisering dat kenmerkend is voor de ontwikkeling van de industriële samenleving en dat grofweg een aanvang neemt aan het begin van de 18de eeuw, voegt daaraan een extra dimensie toe (Beck, 1999). Voor de industriële revolutie worden risico's vooral gezien als gevaren die hun oorsprong vonden in het noodlot en die buiten de invloedsfeer van de mens lagen en eventueel terug te voeren waren op de 'wil van God' (Beck, 1999:50). Gedurende de 19de een 20ste eeuw vindt echter een verandering plaats in de wijze waarop we naar risico's en gevaren kijken. Riskant gedrag wordt gezien als een bron van gevaar en is terug te voeren op de beslissingen die mensen en organisaties bewust of onbewust nemen en die bepaalde onbedoelde gevolgen kunnen hebben, zoals een chemische fabriek in een dichtbevolkt gebied die ondanks allerlei tegenmaatregelen toch ontploft. De gevolgen van deze ontploffing treffen niet alleen de werknemers en de bewoners in de naaste omgeving, maar hebben ook op een grotere schaal ingrijpende gevolgen in termen van bijvoorbeeld lucht, water- en bodemverontreiniging, waardoor ze in verschillende ecosystemen kunnen doordringen, ja zelfs tot in de voedselketen. Volgens Beck (1999: 50) produceert de westerse, kapitalistische samenleving bewust risico's en onzekerheden die vaak onbedoelde, niet voorziene gevolgen hebben; beslissingen die vooral worden ingegeven door overwegingen door doelrationeel handelen ('Zweckrationalität'). Het sterke instrumentele handelen van mensen en de beslissingen die mensen nemen, leidt ertoe dat risico's bewust worden ingecalculeerd. Dit geldt ook voor de afhankelijkheid van ICT-netwerken. Tegelijkertijd leidt de verdere rationalisering van het besluitvormingsproces tot een verdere reductie van risico's tot aanvaardbare risico's. (Beck, 1994: 9). Allerlei maatregelen worden genomen om deze risico's tembaar te maken en daarmee aanvaardbaar, bijvoorbeeld door brandmuren (*firewalls*) aan te leggen tegen hackers en virussen. Toch zegt Beck dat dit niet voldoende is, omdat de netwerksamenleving per definitie een risicosamenleving is. De afhankelijkheden en kwetsbaarheden die hiermee samenhangen zijn per definitie niet te reduceren tot aanvaardbare risico's. Een dergelijke opstelling gaat namelijk voorbij aan de aard van de risico's die samenhangen met het proces van modernisering dat zich al gedurende enkele eeuwen voltrekt. De toegenomen afhankelijkheid en penetratie van ICT-netwerken moet ook in dit licht worden bezien.
Het proces van modernisering dat zich volgens Beck steeds verder ontwikkelt, leidt ertoe dat de (post)-moderne industriële samenleving steeds meer een risico-samenleving wordt, waarbij risico's niet langer meer ingecalculeerd kunnen worden en waarvoor mensen, organisaties en

[9] Hopelijk verandert dat door het *Stappenplan aangifte computercriminaliteit* dat is ontwikkeld binnen het programma Kwint. <http://www.kwint.org/result_files/Stappenplan_Aangifte_Computercriminaliteit.pdf>.

groepen zich niet langer meer afdoende kunnen verzekeren. Er is sprake van een kwalitatieve breuk; een breuk die wordt bespoedigd door een proces dat Beck (1999: 73) 'reflexive modernization' noemt. "The transition from the industrial to the risk epoch of modernity occurs unintentionnally, unseen, compulsively, in the course of a dynamic of modernization which has made itself autonomous, on the pattern unintented consequences".

Oorzaken

Welke factoren die achter dit moderniseringsproces schuilgaan, zorgen ervoor dat risico's niet langer meer als beheersbaar moeten worden beschouwd? Allerlei nucleaire, chemische, ecologische en genetische risico's worden gekenmerkt door het feit dat ze ten eerste niet langer meer beperkt blijven en gelokaliseerd kunnen worden tot een bepaalde plaats en binnen een bepaald tijdsvak, waardoor het aan betekenis verliest. "It becomes an event with a beginning an no end; an 'open-ended festival' of creeping, galloping and overlapping waves of destruction" (Beck, 1999:54,77). Ten tweede is er geen eenduidige relatie tussen oorzaak en gevolg en zijn de schuld- en de aansprakelijkheidsvraag niet eenvoudig te herleiden tot een enkele actor, omdat het veeleer gaat om een diffuus netwerk van wederzijdse afhankelijke actoren die vaak diffuse relaties met elkaar onderhouden (Beck, 1999:53,77). Ten derde zijn er geen afdoende mogelijkheden meer om de geleden schade te kunnen compenseren of te verzekeren. Deze schade is immers immens (Beck, 1999;77). De effecten van deze risico's zijn dusdanig dat ze "undermine or cancel the established safety systems of the welfare state's existing risk calculations" (Beck, 1999:76). De BSE-crisis, en daarmee de problematiek van voedselveiligheid, is in dit verband een voorbeeld van een risico dat Beck bij voorkeur gebruikt om duidelijk te maken in welk type samenleving wij ons thans bevinden. Een ander voorbeeld betreft de aantasting van de ozonlaag door uitstoot van CO_2 en de veronderstelde opwarming van de aarde, met alle gevolgen van dien.

Oplossingsrichting

Hoe gaan wij als samenleving om met de aan dit moderniseringsproces verbonden risico's? Volgens Beck (1999:73) ligt het antwoord in het versterken van de reflexiviteit van het moderniseringproces. "Reflexive modernization means self-confrontation [en geen 'vrijblijvende' reflectie, onze toevoeging] with the consequences of risk society, which cannot (adequately) be addressed and overcome in the system of industrial society (that is measured by society institutionalized standards)". Een noodzakelijke voorwaarde voor de versterking van deze reflexiviteit wordt gevonden in het doorbreken respectievelijk openbreken van het eerder genoemde monopolie waarop risico's worden gedefinieerd. Het is van belang om de zelf-kritiek op de aard van de risicosamenleving te democratiseren. Dit vereist een doorbreking van de bestaande institutionele verhoudingen in onze industriële samenleving – verhoudingen die ervoor zorg dragen dat de politieke betekenis van risico's onvoldoende voor het voetlicht wordt gebracht en die baat hebben bij een economisch-technische benadering van risico's (de zogenaamde 'risico-calculus') waarbij risico's berekend kunnen worden. Zijn ze immers berekend, dan kunnen afdoende maatregelen op grond van een kosten/baten-analyse worden gemaakt (Beck, 1999:77;79).

Het subjectieve karakter van risico's

Met de vraag of we de risico's kennen waarmee we worden geconfronteerd, begint het essay van Douglas & Wildavsky (1982) over *'Risk and culture'*. De facto gaat het niet om het kennen van deze risico's, maar om het beoordelen van bepaalde gebeurtenissen, ontwikkelingen of problemen die mogelijkerwijs risicovol zijn. Het kunnen inschatten c.q. beoordelen van de kans op een bepaald risico wordt bepaald door de wisselwerking van twee factoren, te weten onze kennis over de toekomst en de mate waarin er consensus bestaat over het gewenste toekomstbeeld. Het risicoprobleem in onze westerse samenleving wordt echter bepaald door het feit dat we niet kunnen beschikken over kennis die met zekerheid een beeld geeft van hoe de toekomst eruit ziet. Er is sprake van fundamentele onzekerheid en ambiguïteit. Deze ambiguïteit

wordt nog verder versterkt door het feit dat er geen consensus bestaat over wat de gewenste ontwikkeling van de toekomst is (Douglas & Wildavsky, 1982:5-6). Dit betekent dat "the perception of risk is a social process" (p. 7), hetgeen een sociale theorie van risicoperceptie rechtvaardigt (Douglas & Wildavsky, 1982:7-8). In een dergelijke theorie wordt vooral aandacht gevraagd voor de sociale omgeving waarbinnen bepaalde ontwikkelingen kennelijk wel als risico worden gedefinieerd en andere ontwikkelingen niet als een risico worden beschouwd. Hoe verloopt dit proces van risicoselectie en definitie (Douglas & Wildavsky, 1982:7)? De aanname is dat elke gemeenschap een selectieve kijk heeft op haar natuurlijke omgeving en dat die kijk bepaalt of gevaren al dan niet de moeite waard zijn om tegenmaatregelen te nemen. Dit is een politieke afweging. In de woorden van Douglas & Wildavsky (1984:8) "each social arrangement elevates some risks to a high peak and depresses other below sight. This cultural bias is integral to social organization. Risk taking and risk aversion, shared confidence and shared fears, are part of the dialogue on how best to organize social relations. For to organize means to organize some things in and some things out" . Een culturele analyse van risico's laat vervolgens zien waarom bepaalde zaken wel of niet als een risico worden gezien. Daarbij is van belang hoe bepaalde waarden, belangen en dagelijkse praktijken binnen een specifieke configuratie van actoren de definitie en selectie van risico's bepalen. Omdat de sociale omgeving waarbinnen risico's worden gedefinieerd en geselecteerd kan verschillen, heeft dit ook gevolgen voor de risico's die worden gezien en de maatregelen die worden genomen (Douglas & Wildavsky, 1982:9). Aandacht voor de kwetsbaarheden die samenhangen met de vervlechting van verschillende soorten van infrastructuren was voor de aanslag op de Tweelingtorens in New York op 11 september 2001 nog nauwelijks aanwezig. Daarna zijn we ons als westerse samenlevingen heel bewust geworden van de potentiële gevaren van deze vervlechting. Alleen de Y2K-computerbug (millenniumprobleem) die rondom de wisseling van het millennium in potentie grote delen van het maatschappelijke leven zou kunnen platleggen, had een vonkje van bewustwording laten overslaan. Maar ook hier geldt dat het heel lang heeft geduurd, voordat beslissers overtuigd waren van de dreiging die hiervan uitging.
Geldt dit ook voor individuele organisaties? Hoe bewust zijn zij zich van de risico's van hun afhankelijkheid van ICT-systemen en netwerken? Worden deze risico's ook als risico opgepikt? Voordat deze vraag kan worden beantwoord, is het zinvol om eerst een aantal aspecten van risico's voor het voetlicht te brengen, zoals deze binnen individuele organisaties kunnen worden gelokaliseerd.

4. Aspecten van risico's binnen organisaties

Voor een goed begrip van digitale kwetsbaarheid en van de maatregelen die kwetsbaarheid kunnen verminderen (informatiebeveiliging), waarop verderop wordt ingegaan, is het relevant aandacht te besteden aan waar de meeste risico's nu precies zitten (zie uitgebreid over de diversiteit aan kwetsbaarheden: Neumann, 1995).
In de eerste plaats is het belangrijk te realiseren dat het gevaar niet alleen van buiten komt. Integendeel: uit diverse onderzoeken blijkt dat de meerderheid van beveiligingsincidenten niet wordt veroorzaakt door buitenstaanders, maar door interne medewerkers (vergelijk Neumann, 1995:142). Dat betekent dat beveiliging zich niet alleen, en ook niet in de eerste plaats, moet richten op het oprichten van een elektronische muur om de organisatie, maar ook, en vooral, op interne maatregelen. Aangezien het bij interne medewerkers niet mogelijk is een computersysteem geheel af te sluiten (de meesten moeten immers gebruik kunnen maken van delen van het netwerk), zullen technische maatregelen gecomplementeerd moeten worden met organisatorische maatregelen.
Een tweede aandachtspunt betreft opzettelijke tegenover niet-opzettelijke incidenten. Hoewel men misschien geneigd zou zijn zich te concentreren op bewuste aanvallen op een informatiesysteem, zijn de onbewuste aanvallen vaak minstens even gevaarlijk. Door nalatigheid kan bijvoorbeeld informatie verloren gaan of bekend worden bij ongautoriseerde derden; het hoeft hierbij niet te gaan om exotische incidenten: het omvergooien van een beker hete koffie

over een schootcomputer kan al substantiële gevolgen hebben. En niet alleen de menselijke factor is hier in het spel: grote schade kan worden aangericht door de natuur (zoals een blikseminslag) of door dieren: er zijn diverse gevallen bekend van kamikaze-knaagdieren die elektriciteitskabels doorknaagden, waardoor computersystemen urenlang niet beschikaar waren en computergegevens verloren gingen (Neumann, 1995:7,84-5). Een adequate beveiliging vergt daarom een brede analyse van allerlei mogelijke oorzaken van schade aan informatie- en computersystemen.
Bij een dergelijke analyse moet een derde aandachtspunt worden betrokken: het maakt verschil of een incident gepaard gaat met uitval van kritische systemen of niet. Dat wil zeggen dat naast een analyse van mogelijke oorzaken, ook een analyse van mogelijke gevolgen dient plaats te vinden. Indien een bepaalde oorzaak kan leiden tot onherroepelijke, fundamentele schade, zal de beveiliging groter moeten zijn dan bij minder kritische schade. Een risicoanalyse van digitale kwetsbaarheid moet dus zowel mogelijke oorzaken als mogelijke schades in ogenschouw nemen.

5. De beleidsagenda: voornemens

De overheid heeft een bijzondere verantwoordelijkheid daar waar het de kwetsbaarheden betreft die samenhangen met de aard en de dynamiek van de netwerksamenleving. Omdat onze samenleving alleen maar kan functioneren door en gedragen wordt door ICT-netwerken, raken de risico's die hiermee samenhangen de integriteit en stabiliteit van het normale maatschappelijke verkeer. Het zorgdragen hiervoor kan worden gezien als een van de kerntaken van de overheid. Tegelijkertijd maakt de overheid zelf gebruik van deze infrastructuren voor de uitoefening van haar taken, met name op het terrein van de uitvoering van beleid, toepassing van wet- en regelgeving, de dienstverlening aan burgers, en voor de handhaving en het toezicht op wet- en regelgeving. Burgers, bedrijven, maatschappelijke overheden en andere overheden zijn van de kwaliteit en stabiliteit van deze ICT-infrastructuren afhankelijk. In het Voorschrift Informatiebeveiliging Rijksoverheid (1995) worden eisen gesteld aan de inrichting van de informatiehuishouding binnen overheidsorganisaties. De implementatie van deze voorschriften verloopt echter niet zonder slag of stoot.
In deze paragraaf richten wij ons met name op de beveiliging van de ICT-infrastructuur, zoals die vooral gestalte heeft gekregen in de nota KWINT en de nota Nacotel.

De nota's Kwint en Nacotel

De Nederlandse overheid is zich sinds enkele jaren bewust van de gevaren van een kwetsbare ICT-samenleving. In de nota De Digitale Delta uit juni 1999 werd een verkenning aangekondigd "naar de kwetsbaarheden en zwakheden van de ICT-infrastructuur waarbij speciaal aandacht wordt besteed aan de ontwikkelingen op het gebied van het Internet."[10] De verkenning verscheen in juli 2001: de nota *Kwetsbaarheid op internet (KWINT)*.[11] Hierin zet het kabinet een beleid uiteen op het gebied van ICT-kwetsbaarheid, in het bijzonder rond het Internet.
Parallel aan KWINT is er voorts de actielijn van een Nationaal Continuïteitsplan Telecommunicatie (NACOTEL).[12] Tezamen beogen deze projecten een betrouwbare telecommunicatie-infrastructuur te waarborgen.
Dit beleid kan worden gezien als onderdeel van een ruimer beleid rond vitale infrastructuren, zoals het energienet, waterleidingnetten en de vervoers-infrastructuur. In maart 2001 werd de motie-Wijn aangenomen, die vroeg om een "sectoroverschrijdend plan van aanpak inzake de bescherming van vitale infrastructuur", in het bijzonder in het licht van de groeiende afhankelijkheid van ICT en omdat "de kwetsbaarheid voor vitale maatschappelijke, ICT-

[10] *Kamerstukken II* 1998/99, 26 643, nr. 1; de nota zelf is beschikbaar op <http://www.ez.nl/publicaties/pdfs/05r105.pdf>.
[11] *Kamerstukken II* 2000/01, 26 643, nr. 30.
[12] Zie <http://www.ez.nl/beleid/home_ond/dgtp/veiligheid/nacotel.html>.

afhankelijke diensten groeit".[13] Hoewel de motie de nadruk legde op ICT-afhankelijkheid, gaat de uitvoering veeleer uit van de vitale infrastructuren zelf. In april 2002 werd een grootschalig project Bescherming Vitale Infrastructuren opgezet, met als "opdracht in april 2004 tot stand te hebben gebracht: (1) een samenhangend pakket van maatregelen ter bescherming van de infrastructuur van overheid en bedrijfsleven, waaronder ICT, en (2) de verankering van dat pakket van maatregelen in de normale bedrijfsvoering."[14] Het project richt zich op "vitale sectoren, diensten en producten die bij uitval of verstoring nationale impact hebben",[15] waarbij het meer gaat om het waarborgen van continuïteit van de normale bedrijfsprocessen van vitale infrastructuur dan om het beveiligingsaspect als zodanig.[16] Het project zal leiden tot voorstellen voor een pakket beschermingsmaatregelen, dat in april 2004 aan de Tweede Kamer wordt aangeboden.[17]
Vanwege de gerichtheid van dit hoofdstuk op ICT-kwetsbaarheid, en het vooralsnog ontbreken van concrete beleidsvoorstellen in het bredere vitale-infrastructurenproject, beperken wij ons in het navolgende tot de actielijn van KWINT.

De rol van de overheid
Volgens de nota KWINT kan het Internet worden beschouwd als één van de kritieke infrastructuren van Nederland.[18] Gezien het toenemende aantal incidenten die de kwetsbaarheid van het Internet aantonen, is het van vitaal belang dat beschermingsactiviteiten worden ondernomen. Het kabinet zet in de nota KWINT uiteen aan welke activiteiten wordt gedacht, en wat de rollen zijn van de diverse partijen die daarbij betrokken zijn.
Hoewel de nota primair uitgaat van overheidsactiviteiten, is de rol van de overheid bescheiden. De primaire verantwoordelijkheid voor beveiliging ligt bij elke partij zelf, en de overheid beperkt zich vooralsnog tot het in de gaten houden van ontwikkelingen en het uitvoeren van een faciliterende rol, met terughoudendheid in regelgeving "om de zich nog ontwikkelende markt niet onnodig te verstoren".[19] Publiek-private samenwerking, zowel nationaal als internationaal, staat voorop.
Vanuit deze visie op de rol van de overheid, beschrijft de nota vervolgens acht actielijnen, deels activiteiten die al werden ondernomen, deels nieuwe onderwerpen:
1. voorlichting;
2. onderzoek en ontwikkeling;
3. beveiligingsbeleid en –maatregelen binnen een organisatie;
4. exclusiviteit van informatie;
5. transparantie door kwaliteitsgegevens;
6. alamering en incident response;
7. integriteit van informatie;
8. cybercrime.

Deze actielijnen vormen een nogal ongelijksoortig geheel dat enigszins willekeurig overkomt. Zo staan er twee beveiligingsdoelen tussen, exclusiviteit (vertrouwelijkheid) en integriteit, maar de derde – beschikbaarheid – ontbreekt (dit doel is alleen opgenomen onder de noemer van kwaliteitsgegevens: internetaanbieders dienen transparant te maken welk beschikbaarheidsniveau zij halen). Deze doelen staan tussen bedreigingen (cybercrime) en maatregelen, zowel generieke (voorlichting, onderzoek & ontwikkeling, alarmering) als individuele (stimuleren van organisatiebeleid).

[13] *Kamerstukken II* 2000/01, 26 643, nr. 20.
[14] *Kamerstukken II* 2002/03, 26 643, nr. 39.
[15] *Kamerstukken II* 2002/03, 26 643, nr. 39, p. 2.
[16] *Kamerstukken II* 2002/03, 26 643, nr. 40, p. 9.
[17] *Kamerstukken II* 2002/03, 26 643, nr. 42.
[18] *Kamerstukken II* 2000/01, 26 643, nr. 30, p. 4.
[19] *Kamerstukken II* 2000/01, 26 643, nr. 30, p. 4.

Als geheel biedt de nota KWINT wel de nodige plannen om de kwetsbaarheid van het Internet te verminderen; zinvol zijn bijvoorbeeld de maatregelen om bedrijven te stimuleren een beveiligingsbeleid en –maatregelen te treffen, en het oprichten door BZK van een CERT (Central Emergency Respons Team) voor de overheid. Maar door het gebrek aan een rode draad of zichtbare logica in de actielijnen, alsmede door de terughoudende rol die de overheid op zich neemt, blijft het beleid enigszins steken in goede bedoelingen en het opsommen van activiteiten die toch al plaatsvonden. Tegelijkertijd moet worden geconstateerd dat in de nota KWINT risico's vooral worden geïdentificeerd binnen het domein van het internet en dat de voorgestelde acties vooral binnen dit domein plaatsvinden. Er is echter maar weinig aandacht voor de risico's die samenhangen met de vervlechting van sociaal-organisatorische, fysieke en ICT-netwerken en infrastructuren (Bekkers e.a., 2002).

Men kan zich afvragen of de overheid niet een meer sturende en actieve rol op zich zou moeten nemen. Het is vanzelfsprekend dat partijen een eigen verantwoordelijkheid hebben en dat de ontwikkeling van het Internet voor een groot deel te danken (en soms te wijten) is aan private ondernemingen. Echter, waar de praktijk tot nu toe lijkt uit te wijzen dat er systematisch gebrek is aan structurele informatiebeveiliging en waar duidelijk is dat de ICT-infrastructuur een vitaal en kwetsbaar onderdeel is van de Nederlandse samenleving, is het de vraag of een afwachtende houding aanvaardbaar is. Het is zeer de vraag of 'de markt' voldoende toegerust is om een adequate bescherming te bieden tegen alle vormen van ICT-kwetsbaarheid; zoals eerder als is opgemerkt kost informatiebeveiliging immers structureel geld zonder zichtbare baten. Het risico bestaat dat publiek-private samenwerking, waarbij de maatregelen primair moeten komen van de private sector met enige facilitering door de overheid, onvoldoende robuust is om de vele bedreigingen van de infrastructuur en ICT-voorzieningen het hoofd te bieden. Hiermee is niet gezegd dat de overheid in alles het voortouw moet nemen, maar wel dat de overheid zich – meer dan in de nota KWINT gebeurt – rekenschap dient te geven van de noodzaak van concrete en adequate maatregelen om de ICT-infrastructuur te beschermen. Dit publieke belang vraagt om substantiële publieke inzet en hoge prioritering op de politieke agenda. Daarbij is het tevens van belang dat de overheid zichtbaar maakt dat zij de eisen die ze aan de private sector stelt, ook zelf waarmaakt. Zij heeft daarin een belangrijke voorbeeldrol te vervullen.

6. De organisatorische en technische agenda: maatregelen

Het overheidsbeleid zoals geschetst in de vorige paragraaf, leunt in belangrijke mate op een aantal fundamentele maatregelen die genomen kunnen worden om ICT-kwetsbaarheid te verminderen of binnen de perken te houden. In deze paragraaf gaan wij nader in op deze maatregelen.
Een adequate beveiliging dient rekening te houden met alle risico's, dat wil zeggen met mogelijke oorzaken en mogelijke gevolgen van ICT-kwetsbaarheid. Voor het opstellen van een beveiligingsplan zijn diverse hulpmiddelen beschikbaar; de belangrijkste daarvan is de *Code voor informatiebeveiliging* (2000), een norm voor informatiebeveiliging. Deze geeft inzicht in de totstandkoming van en eisen voor een beveiligingsplan. Het belangrijkste onderdeel van zo'n plan zijn de concrete maatregelen die in de specifieke context van de organisatie moeten worden genomen. In deze paragraaf gaan wij nader in op de mogelijke maatregelen die kunnen worden getroffen.

6.1. Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het door middel van technische, organisatorische en juridische instrumenten beveiligen van informatie(systemen) en informatiestromen in en tussen organisaties. Het doel van informatiebeveiliging is – vanuit organisatieoogpunt – het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van schade voor organisaties door het trachten te voorkomen van beveiligingsincidenten en het minimaliseren van de eventuele gevolgen (Code voor Informatiebeveiliging, 2000). Daarnaast zullen ook particulieren

maatregelen op gebied van informatiebeveiliging willen treffen om (directe of gevolg-)schade aan PC's en persoonlijke informatie(bestanden) te voorkomen.
Informatiebeveiliging maakt het mogelijk om informatie in groepen in en tussen organisaties te gebruiken zonder dat de integriteit van de informatie wordt aangetast of op zijn minst de mogelijkheid van aantasting wordt verkleind. Met name de laatste jaren is de behoefte aan en het belang van informatiebeveiliging enorm toegenomen.

Bij informatiebeveiliging worden drie basisbeginselen onderscheiden, te weten (1) beschikbaarheid, (2) vertrouwelijkheid, en (3) deugdelijkheid.[20]
(1) *Beschikbaarheid* ziet op het garanderen dat gegevens en diensten op de juiste momenten beschikbaar zijn voor gebruikers.
(2) *Vertrouwelijkheid* betreft het beschermen van gegevens (bijvoorbeeld bedrijfsgeheimen of persoonsgegevens) tegen onbevoegde kennisname.
(3) *Deugdelijkheid* gaat over het waarborgen van de juistheid en volledigheid van gegevens (integriteit en authenticiteit) en de correcte werking van informatiesystemen (systeemintegriteit).

De instrumenten van informatiebeveiliging kunnen worden onderverdeeld in drie categorieën: (1) technische middelen, (2) organisatorische maatregelen en (3) juridische maatregelen (zie nader Van Kralingen & Kolkman, 1998:209-211).
(1) Primair technische maatregelen komen neer op het inzetten van technische (hulp)middelen. Voorbeelden van technische hulpmiddelen zijn op encryptie gebaseerde technieken, zoals *Secure Socket Layer* (SSL) en digitale handtekeningen (en certificaten), maar ook vuurmuren (*firewalls*), het gebruik van PIN-codes en biometrische technieken.
(2) Bij primair organisatorische maatregelen gaat het om interne of externe maatregelen ten behoeve van de inrichting en het functioneren van organisaties. Gedacht kan worden aan het geven van voorlichting, het ontwikkelen van interne beveiligings- en autorisatieprocedures en het (laten) uitvoeren van EDP (*Electronic Data Processing*) *audits*, maar ook het gebruiken van een *Public Key Infrastructure* (PKI) en het certificeren van programmatuur.
(3) Bij juridische maatregelen gaat het vaak om afspraken tussen partijen, zoals overeenkomsten, *interchange agreements* en algemene voorwaarden, maar ook bijvoorbeeld mandaatregelingen, waarbij intern bevoegdheden worden toebedeeld. Ook is er sprake van juridische maatregelen bij (internationale) richtlijnen of voorbeeldwetgeving, zoals de UNCITRAL-*Model Law on Electronic Commerce*.
Men dient hierbij voor ogen te houden dat maatregelen nooit op zichzelf staan. Een technische maatregel is zelden zinvol als niet tegelijkertijd organisatorische maatregelen worden getroffen; zo is een wachtwoordbeveiliging erg kwetsbaar als de meerderheid van de gebruikers de naam hun kind, partner, voetbalclub of automerk hanteert.[21] Omgekeerd gaan organisatorische maatregelen altijd gepaard met enige vorm van techniek, zoals logging van gegevensstromen om controleprocedures mogelijk te maken. Waar we in de volgende paragraaf ingaan op de belangrijkste technische en organisatorische maatregelen, moet men zich dus realiseren dat elk middel in principe zowel technische als organisatorische, en soms ook juridische, maatregelen omvat.

[20] Wij hanteren de term deugdelijkheid als koepelterm voor integriteit en authenticiteit. De BVD van informatiebeveiliging weerspiegelt aldus de in de literatuur gebruikelijke verwijzing naar de "CIA of information security": *confidentiality*, *integrity* en *availability*.
[21] Onderzoek Safe Internet Foundation & PWC, 7 juli 2003, *de Volkskrant* 8 juli 2003.

6.2 Primair technische maatregelen

6.2.1. Cryptografie

A. Technische context

Systemen voor het versleutelen van gegevens bestaan al sinds de Oudheid. Tot de jaren zeventig van de vorige eeuw waren al die systemen gebaseerd op een principe dat één en dezelfde, geheime sleutel moest worden uitgewisseld tussen communicatiepartners. Dat had als nadeel dat die sleutel dus op een betrouwbare manier moet worden overgebracht, bijvoorbeeld met de (slakken)post, een koerier of in persoon. Waar dat op kleine schaal goed mogelijk is, is zo'n systeem op grote schaal slecht toepasbaar, zeker voor een e-handelaar die met veel klanten veilig wil communiceren.

Om het probleem van sleuteluitwisseling op te lossen, is in de jaren zeventig een andere vorm van cryptografie uitgevonden: de asymmetrische cryptografie. Asymmetrische cryptografie gaat uit van het principe dat elke gebruiker twee sleutels heeft: een openbare of publieke[22] en een privésleutel[23]. Elke gebruiker verspreidt haar openbare sleutel onder potentiële communicatiepartners; de privésleutel houdt zij strikt geheim. De privésleutel wordt normaliter opgeslagen op een gegevensdrager (harde schijf of diskette), beveiligd met een (moeilijk te raden) wachtwoord. Ambtenaar Annie en burger Bob kunnen nu als volgt veilig communiceren. Bob zoekt Annie's openbare sleutel op op haar weblocatie en versleutelt daarmee een bericht. Hij stuurt het bericht naar Annie, die het vervolgens ontcijfert met haar corresponderende privésleutel. Buurvrouw Coba kan het bericht niet ontcijferen als zij het zou onderscheppen, omdat zij Annie's privésleutel niet kent.

Een analogie kan dit verduidelijken. Annie gebruikt vertaling in het Koeterwaals als haar cryptosysteem. Ze heeft een publieke sleutel: het woordenboek Nederlands-Koeterwaals, en een privésleutel: het woordenboek Koeterwaals-Nederlands. Bob versleutelt een boodschap aan Annie door met het woordenboek Nederlands-Koeterwaals het bericht in het Koeterwaals te vertalen. Annie kan het vervolgens lezen door het terug te vertalen naar het Nederlands. Omdat zij de enige is met een woordenboek Koeterwaals-Nederlands, blijft de boodschap voor alle anderen Koeterwaals. Iemand kan weliswaar de moeite nemen om bij elk woord Koeterwaals het (openbare) woordenboek Nederlands-Koeterwaals te gebruiken om te kijken bij welk Nederlands woord dit hoort, maar dit is in de praktijk – zeker bij de Dikke Koeterwaals – praktisch onmogelijk.

De crux van het beveiligen met cryptografie berust op de volgende principes: een robuust systeem dat zijn veiligheid in de praktijk bewezen heeft (en liefst openbaar is zodat het geen verborgen achterdeuren kan bevatten), een sleutel van voldoende lengte, en een zorgvuldige omgang door de gebruikers met het wachtwoord dat de privésleutel beveiligt.[24]

Vooral dat laatste is een zwakke schakel bij de beveiliging. De privésleutel – de naam zegt het al – mag slechts bekend zijn aan de houder van het sleutelpaar dan wel andere bevoegde gebruikers. Voor een correcte en betrouwbare werking is het derhalve van belang dat de houder de sleutel niet toegankelijk voor anderen laat "rondslingeren". Vaak zal de sleutel zijn beveiligd met behulp van een wachtwoord of een PIN-code die slechts bekend hoort te zijn aan de houder van de sleutel of andere geautoriseerde gebruikers. Het is dan ook van belang een dergelijk wachtwoord

[22] Een publieke sleutel is de openbare helft van een encryptiesleutelpaar die verspreid wordt onder communicatiepartners. Hiermee kan een digitale handtekening gecontroleerd worden. Ook kan hiermee een bericht worden versleuteld om het voor onbevoegden onleesbaar te maken (alleen de houder van de bijbehorende privésleutel kan het ontsleutelen) (Koops & Van der Wees, 1998:233-4).

[23] Een privésleutel is de helft van een encryptiesleutelpaar die door de bezitter strikt geheim gehouden moet worden. Hiermee kan een digitale handtekening gemaakt worden. Ook kan de sleutel gebruikt worden om versleutelde berichten leesbaar te maken (Koops & Van der Wees, 1998:233-4).

[24] Zie verder over techniek en gebruik van cryptografie de standaardwerken Schneier, 1996, en Menezes, Van Oorschot & Vanstone, 2001, en meer inleidend Garfinkel, 1997, deel IV.

niet te noteren of tegen onbevoegden te vermelden, terwijl ook niet een makkelijk te raden wachtwoord mag worden gekozen (zoals een woord uit het woordenboek). Ook is het aan te bevelen de apparatuur waarop de sleutel is opgeslagen, zoals een PC of een smartcard, te beveiligen of veilig op te bergen. De publieke sleutel moet in tegenstelling tot de private sleutel publiekelijk worden bekend gemaakt, waarbij een certificatenaanbieder (CA) behulpzaam kan zijn – een TTP (zie onder).

Voor netwerken van specifiek belang zijn twee cryptoprotocollen die veel worden gebruikt. SET (Secure Electronic Transactions) verzorgt het veilig versturen van kredietkaartnummers.[25] SSL (Secure Sockets Layer) is een methode om gestandaardiseerd versleutelde en geauthenticeerde berichten over het Internet te versturen. Als de server van een dienst- of informatieaanbieder SSL heeft geïmplementeerd, kan het bladerprogramma van de afnemer zorgen voor versleutelde communicatie met deze aanbieder (herkenbaar aan het voorvoegsel 'https', met de s van 'secure').[26]

Organisatorische context

Organisaties die cryptografie gebruiken voor vertrouwelijkheid, beveiligen hun gegevens tegen onbevoegde kennisname. Als dat goed gebeurt, lopen zij evenwel een risico. Indien de rechtmatige gebruiker de sleutel kwijtraakt of het wachtwoord vergeet, of als een werknemer die de vertrouwelijke gegevens versleuteld heeft opgeslagen plotseling verdwijnt, kan de organisatie zelf ook niet meer ontsleutelen – de gegevens zijn dan onherroepelijk verloren.
Om aan dit risico tegemoet te komen, zijn systemen ontwikkeld voor gegevensherwinning (*data recovery*). Door een kopie van de privésleutel op te slaan op een vertrouwde, beveiligde plaats, of door systemen te gebruiken waarbij sessiesleutels kunnen worden achterhaald, kan de rechtmatige gebruiker dan alsnog bij de gegevens, ook al is zij de benodigde sleutel kwijt.
Een mogelijke instantie om dergelijke gegevens op te slaan, is een Trusted Third Party (TTP) die fungeert als sleutelbeheerder (*Key Escrow Agent*), dat wil zeggen een vertrouwde derde die (kopieën van) ecryptiesleutels in bewaring houdt. Een TTP kan ook een zogeheten gegevensherwinner (Data Recovery Organisation, DRO) zijn. Een DRO garandeert dat versleutelde gegevens toegankelijk blijven voor bevoegden, ook indien de ontcijfersleutel niet (meer) beschikbaar is.
Een DRO kan sleuteldepot (*key escrow*) of sleutelherwinning (*key recovery*) gebruiken. Gegevensherwinning is een techniek waarbij per bericht de ontcijfersleutel toegankelijk is voor de TTP. In tegenstelling tot sleuteldepot is bij gegevensherwinning niet de privésleutel toegankelijk, maar de sessiesleutel. Een sessiesleutel is een symmetrische sleutel die één keer wordt gebruikt voor een berichtenuitwisseling of een telefoongesprek en nadat de sessie is afgelopen wordt weggegooid (Koops & Van der Wees, 1998:233-4).
Dergelijke systemen hebben zich echter in de praktijk nog niet echt bewezen, en ze brengen ook extra veiligheidsrisico's met zich mee. Er zijn dan ook nauwelijks publieke TTP's op de markt voor dit soort diensten. Wel vindt gegevensherwinning vaker plaats intern, door een intern afgeschermde eenheid aan te wijzen als gegevensherwinner. Ook daarbij moet men zich echter realiseren dat een herwinningsmogelijkheid tegelijkertijd een extra mogelijkheid betekent voor derden om kennis te nemen van beveiligde gegevens; natuurlijk valt dit wel te beveiligen, maar dat kan aanzienlijke kosten met zich mee brengen (denk aan het inhuren van gescreend personeel en aan toezichtprocedures). Men moet daarom een afweging maken tussen het risico versleutelde gegevens kwijt te raken en het risico van extra veiligheidslekken (zie nader Koops & De Jong, 1998).

[25] Zie <http://www.sans.org/infosecFAQ/covertchannels/SET.htm> en <http://www.setco.org/set.html>.
[26] Zie <http://developer.netscape.com/tech/security/ssl/protocol.html> en Garfinkel, 1997, hfd. 12 over SSL.

Mocht het nog onverhoopt misgaan, dan zijn er nog gespecialiseerde bedrijfjes[27] om versleutelde gegevens weer toegankelijk te maken (maar als die slagen, dan zaten er kennelijk zwaktes in de beveiliging!).

Juridische context
Cryptografie is een noodzakelijk onderdeel van informatiebeveiliging. Het kan echter ook worden gebruikt voor minder nobele doelen, bijvoorbeeld door misdadigers om de politie dwars te zitten. Van oudsher hebben overheden beperkingen opgelegd aan de export van cryptografie, en over regulering van het verhandelen en gebruik van cryptografie wordt nog druk nagedacht (zie Koops, 2002, en daar weergegeven bronnen).
Sinds de Koude Oorlog bestaan er wereldwijde afspraken over de export van cryptografie. Het huidige Wassenaar Akkoord is een overeenkomst tussen 33 landen die de export van wapens aan banden legt; cryptografie wordt beschouwd als een goed voor tweeërlei gebruik (militair en civiel) en wordt ook beperkt.[28] Dit geldt overigens alleen voor de export van cryptografiesystemen zelf; men mag wel vrijelijk versleutelde berichten 'exporteren'. De meeste Westerse landen hebben de afspraken omgezet in hun nationale wetgeving.
Hoewel de exportbeperkingen geleidelijk aan worden versoepeld, is er voor export van sterke cryptografie in het algemeen nog steeds een vergunning nodig. Binnen de EU is de export echter vrij.[29] Internationaal opererende organisaties die vertrouwelijk met het buitenland willen communiceren, moeten aandacht besteden aan de voorwaarden waaronder cryptografie vanuit die landen mag worden geëxporteerd.
Exportbeperkingen betekenen niet een verbod op export. In de meeste gevallen is het wel mogelijk cryptografie te exporteren, mits men daarvoor een vergunning heeft. Dergelijke vergunningen moet men aanvragen bij de nationale bevoegde instanties. Voor Nederland is dat de Afdeling Exportcontrole en Sanctiebeleid van het Ministerie van EZ.[30]

Overigens is *import* van cryptografie in het algemeen geen probleem; slechts enkele landen, waaronder vooralsnog ook Frankrijk, leggen daarvoor beperkingen op.

6.2.2 Elektronische handtekeningen & PKI

Technische context
Een elektronische handtekening is een authenticatievorm via elektronische weg. Dit kan vele vormen aannemen: een ingescande handtekening, een ingetikte naam, een handtekening met een elektronische pen die de volgorde en druk van de handtekening meet, een irisscan of digitale vingerafdruk. De tot nu toe meestgebruikte en betrouwbaarste vorm van de elektronische handtekening is echter de digitale handtekening, die is gebaseerd op de techniek van asymmetrische encryptie (zie 6.2.1, onder A). Wij beperken ons daarom in deze paragraaf tot deze vorm van elektronische authenticatie; biometrie komt in de volgende paragraaf aan de orde.

De digitale handtekening werkt eveneens met behulp van een publiek-privaat sleutelpaar. Bob – de sleutelhouder – kan nu met zijn privésleutel een uittreksel (*digest* of *hash*) van een bericht versleutelen. Dit versleutelde uittreksel voegt hij toe aan het bericht en hij verstuurt het geheel aan geadresseerde Annie. Zij kan vervolgens met behulp van de publieke sleutel van Bob controleren of het bericht inderdaad van hem afkomstig is: als Bobs publieke sleutel werkt op het

[27] Zoals <http://www.accessdata.com/>.
[28] Zie <www.wassenaar.org>.
[29] Council Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology, *OJ* L159, 30 January 2000.
[30] Zie <http://cwis.kub.nl/~frw/people/koops/cls-addr.htm> voor een overzicht van adressen van exportinstanties.

versleutelde uittreksel in combinatie met het ondertekende bericht, moet het zijn versleuteld met de privésleutel van Bob. Daarmee kan Annie tegelijk controleren of het bericht onderweg niet door buurvrouw Coba of fraudeur Frits is veranderd.

De digitale handtekening heeft aldus twee functies, te weten het waarborgen van de *integriteit* van elektronische berichten alsmede het garanderen van de *authenticiteit* in het communicatieverkeer. Met het eerste wordt bedoeld dat kan worden gecontroleerd of berichten tijdens het transport over het netwerk zijn gewijzigd (lees: gemanipuleerd). Het tweede betekent dat kan worden geverifieerd van wie een elektronisch bericht of document afkomstig is. Tevens zal hiermee vaak ook een authenticatie van de inhoud worden bewerkstelligd, maar dat hoeft niet per definitie het geval te zijn. Er zijn ook *blind signatures* waarbij de tekenende instantie niet op de hoogte is van de inhoud van het bericht. Blinde handtekeningen vinden bijvoorbeeld toepassing bij de uitgifte van elektronisch geld (*e-cash*), opdat de bank wel kan controleren dat een betaling correct is maar niet wie de betaler is.

Overigens kan een digitale handtekening ook in combinatie met encryptie voor vertrouwelijkheid worden gebruikt, door eerst de vertrouwelijkheid te garanderen (met de publieke sleutel van de ontvanger) en vervolgens het bericht te ondertekenen (met de privésleutel van de afzender).

Organisatorische context
De betrouwbaarheid van digitale handtekeningen op zichzelf is niet groot: iedereen kan immers een sleutelpaar aanmaken op naam van iemand anders – er is niets inherent persoonlijks aan een digitale handtekening. Daarom zijn aanvullende organisatorische maatregelen nodig, namelijk een certificatieaanbieder en een publieke-sleutel-infrastructuur (PKI).
Een certificatiedienstverlener of Certification Authority (CA) is een vertrouwde instantie die publieke sleutels certificeert en digitale certificaten[31] publiceert ten behoeve van digitale handtekeningen; indien gewenst kan de CA ook zelf de sleutelparen aanmaken.
Bij de digitale handtekening is het noodzakelijk om houder en publieke sleutel op een betrouwbare wijze aan elkaar te verbinden. Anders zou Frits immers een sleutelpaar kunnen aanmaken op naam van Bob en daarmee bij Annie digitale diensten afnemen op kosten van Bob. Het creëren van een band tussen houder en publieke sleutel gebeurt door middel van digitale certificaten die door een CA worden uitgegeven na controle van de identiteit en/of hoedanigheid van de houder en van diens bezit van de bijbehorende privésleutel.
Over het algemeen zal een CA ook een zogeheten *Revocation Service* aanbieden, oftewel een dienst waarbij certificaten worden ingetrokken bij de beëindiging van de overeenkomst, het aflopen van de geldigheidsduur van het certificaat, de constatering van fouten in het certificaat of bij het uitlekken van de privésleutel die hoort bij de in het certificaat opgenomen publieke sleutel. De ingetrokken certificaten worden opgenomen in een online databank, de *Certificate Revocation List*. Gebruikers van digitale handtekeningen behoren deze lijst te raadplegen alvorens op een digitale handtekening te vertrouwen.
CA's maken over het algemeen onderdeel uit van een *Public Key Infrastructure* (PKI). Een PKI is een hiërarchische of horizontale structuur van CA's waarbinnen architectuur, organisatie, gebruikte techniek, gebruiken en procedures op elkaar zijn afgestemd en waarbij CA's elkaar certificeren. Een PKI verstevigt aldus het vertrouwen in de CA en in de digitale handtekeningen binnen de infrastructuur.
De Nederlandse overheid is in 1999 begonnen met de ontwikkeling van een PKI voor betrouwbare communicatie binnen en met de Nederlandse overheid onder de naam

[31] Een digitaal certificaat is een digitaal document dat de binding van een (natuurlijk of rechts-) persoon met een publieke encryptiesleutel garandeert, uitgegeven door een Certificatenaanbieder (CA). Het certificaat bevat tenminste de publieke sleutel van de persoon, de unieke naam van de persoon, een geldigheidsdatum en gegevens over de CA. Het geheel is door de CA ondertekend met diens privésleutel, waardoor de gegevens niet manipuleerbaar zijn (Koops & Van der Wees, 1998:233-4).

PKIoverheid.[32] De taskforce PKIoverheid bestaat uit een informatiecentrum PKI (iPKI), dat voorlichting en ondersteuning bij de invoering van PKI voor de overheid geeft, alsmede uit de Tijdelijke Policy Authority PKIoverheid (TPA), die werkt aan de inrichting van de *Policy Authority* die verantwoordelijk is voor het ondersteunen van de Minister van BZK bij het beheer over de overheidsPKI. PinkRoccade heeft de primeur met de goedkeuring van de *Policy Authority* om als certificatiedienstverlener gekwalificeerde certificaten binnen de PKI voor de overheid uit te geven.[33] Inmiddels lopen er reeds verschillende proefprojecten bij onder meer ministeries, zelfstandige bestuursorganen en de Vereniging van Kamers van Koophandel, waarbij elektronische handtekeningen ten behoeve van een betrouwbaar communicatieverkeer worden ingevoerd.[34]

Juridische context

De elektronische handtekening is sinds jaren onderwerp van veel regulering wereldwijd om ervoor te zorgen dat de techniek toelaatbaar is als bewijs en kan worden gebruikt voor het rechtsgeldig ondertekenen van elektronische overeenkomsten.[35] In de Europese lidstaten wordt de richtlijn 1999/93/EG inzake elektronische handtekeningen geïmplementeerd. Deze richtlijn ziet op de toelaatbaarheid van elektronische handtekeningen als bewijs en niet op het rechtsgeldig ondertekenen van elektronische overeenkomsten (artikel 1). De rechtsgeldigheid van elektronische contracten wordt bestreken door artikel 9 richtlijn 2000/31/EG inzake elektronische handel.

Richtlijn 1999/93/EG is op het eerste gezicht gericht op elektronische handtekeningen meer in het algemeen en beoogt een juridische gelijkstelling te bereiken met handmatige handtekeningen. De regeling maakt onderscheid tussen gewone elektronische handtekeningen en geavanceerde elektronische handtekeningen. Onder 'elektronische handtekening' worden begrepen: "elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie"[36] (artikel 2 onder 1). Een geavanceerde elektronische handtekening is "een elektronische handtekening die voldoet aan de volgende eisen: a) zij is op unieke wijze aan de ondertekenaar verbonden; b) zij maakt het mogelijk de ondertekenaar te identificeren; c) zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en d) zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord" (artikel 2 onder 2). De digitale handtekening zal over het algemeen voldoen aan de eisen van een geavanceerde e-handtekening.

De geavanceerde e-handtekening ofwel digitale handtekening die is gebaseerd op een gekwalificeerd certificaat[37] en door een veilig middel is aangemaakt, wordt in de richtlijn gelijkgesteld aan de handmatige handtekening. De gewone elektronische handtekening kent een zwakkere status en mag noch rechtsgeldigheid worden ontzegd noch worden geweigerd als bewijsmiddel voor de rechter op het grond van het enkele feit dat de handtekening in elektronische vorm is gesteld, niet is gebaseerd op een gekwalificeerd certificaat, niet is gebaseerd op een door een geaccrediteerde CA afgegeven certificaat of niet met een veilig middel is aangemaakt (alles artikel 5).

[32] Zie <http://www.pkioverheid.nl>.
[33] Zie <http://www.pinkroccadecsp.nl/> en <http://www.opta.nl/index.asp?url=/nieuwsenpublicaties/document.asp&id=1178>.
[34] Zie Netkwesties, editie 59, http://<http://www.netkwesties.nl/editie59>.
[35] Zie Van der Hof, 2003, voor een overzicht van regulering en Aalberts & Van der Hof, 2000, voor verschillende benadering in digitalehandtekeningenregulering.
[36] 'Authentificatie' is de term in de officiële Nederlandse vertaling maar is geen bestaand Nederlands woord. Wij gebruiken liever het reeds bestaande 'authenticatie'.
[37] Een gekwalificeerd certificaat is een digitaal certificaat dat voldoet aan specifieke, door de richtlijn gestelde eisen en is uitgegeven door een CA die tevens aan door de richtlijn gestelde criteria van betrouwbaarheid, veiligheid en deskundigheid voldoet (artikel 2 onder 10).

In het kader van het TTP.NL[38] project zijn randvoorwaarden voor onder andere TTP's die CA-functies uitoefenen opgesteld. De randvoorwaarden hebben voornamelijk betrekking op de betrouwbaarheid van CA's en omvatten factoren als beveiliging, bedrijfscontinuïteit, rechtmatig handelen, betrouwbare technologie, functiescheiding, toezicht en transparantie.[39]
Hoewel de juridische inkadering van de elektronische handtekening vooralsnog primair in het privaatrecht heeft plaatsgevonden, is deze context niettemin relevant voor de overheid. Artikel 3:15c BW bepaalt namelijk dat de bepalingen van Afdeling 3.1.1A van het Burgerlijk Wetboek overeenkomstige toepassing vinden buiten het vermogensrecht, voorzover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet. In dit verband is het interessant te kijken naar het voorstel voor een Wet elektronisch bestuurlijk verkeer, dat beoogt de Algemene wet bestuursrecht aan te vullen met regels over verkeer langs elektronische weg tussen burgers en bestuursorganen.[40] In ontwerpartikel 2:16 wordt bepaald dat "aan het vereiste van ondertekening is voldaan door een elektronische handtekening, indien de methode die daarbij voor authentificatie is gebruikt voldoende betrouwbaar is, gelet op de aard en de inhoud van het elektronische bericht en het doel waarvoor het wordt gebruikt." In de daaropvolgende zin worden artikel 3:15a leden 2 tot en met 6 en artikel 3:15b BW van overeenkomstige toepassing verklaard. Tevens kunnen bij wettelijk voorschrift aanvullende eisen worden gesteld. Op basis van richtlijn 1999/93/EG inzake elektronische handtekeningen hebben lidstaten de mogelijkheid om verdergaande vereisten te stellen aan het gebruik van elektronische handtekeningen in de openbare sector. Deze eisen moeten, zo stelt de richtlijn in artikel 3 lid 7, objectief, transparant, evenredig en niet-discriminerend zijn en mogen slechts op de specifieke kenmerken van de betrokken toepassing betrekking hebben. Zij mogen verder geen belemmering vormen voor grensoverschrijdende diensten.

6.2.3. Biometrie[41]

Biometrie is zowel een herkennings- als een beveiligingsmethode. Als herkenningsmiddel kent het verschillende functies, waaronder verificatie van de identiteit van een persoon en daarmee samenhangend authenticatie en autorisatie. Biometrie kan ook worden gebruikt voor beveiliging *zonder* identificatie, door de toegang tot een systeem te beperken tot degene van wie het biometrische kenmerk overeenkomt met het kenmerk dat in het systeem of op een *smart card* is opgeslagen.

Technische context
Biometrie is een techniek die gebruik maakt van persoonskenmerken, zoals fysieke of gedragskenmerken. Op fysieke kenmerken gebaseerde biometrische methoden zijn onder meer identificatie door middel van iris- of gezichtsherkenning, het gebruik van vingerafdrukken en handgeometrie. Van gedragskenmerken wordt gebruik gemaakt bij de digitale pen. Bij deze methode worden druk en snelheid tijdens het tekenen gemeten en getoetst aan de voor de desbetreffende persoon in een database opgeslagen waarden. Het bijzondere aan biometrie is dat de gebruikte persoonskenmerken – naast het feit dat ze uniek zijn – niet kunnen worden vergeten, verloren of overgedragen.[42]

[38] Dit is een project, ondergebracht bij ECP.NL, waarbinnen diverse personen uit bedrijfsleven en overheid hebben samengewerkt aan de ontwikkeling van randvoorwaarden waaronder Trusted Third Parties goed zouden kunnen functioneren in Nederland. Zie <http://www.ecp.nl/dossieritem.php?dossier_id=7>.
[39] Beleidsnotitie Nationaal TTP-Project, Min. V&W, Min. EZ, maart 1999, p. 17-22.
[40] *Kamerstukken II* 2001/02, 28 483, nrs. 1-2.
[41] Deze paragraaf is grotendeels gebaseerd op Van Kralingen, Prins & Grijpink, 1997.
[42] Wel kan een persoon onder bedreiging gedwongen worden haar persoonskenmerk te gebruiken, zodat misbruik niet volledig is uitgesloten. De in de literatuur met zekere wellustigheid genoemde voorbeelden van afgehakte vingers laten wij hier buiten beschouwing: een goed biometrisch product reageert niet op dode lichaamsdelen.

Een biometrisch kenmerk wordt (meermaals) ingelezen door een sensor. Vervolgens worden de onderscheidende gegevens van het biometrisch kenmerk gedigitaliseerd en omgezet in een reeks cijfers. Deze reeks wordt opgeslagen in een *template* dat vervolgens wordt gebruikt in het herkenningssysteem of de *smart card*. Tijdens de verificatie met behulp van het herkenningssysteem of de *smart card* wordt het proces van inlezen en digitaliseren herhaald en wordt het resultaat vergeleken met de in het systeem of op de *smart card* opgeslagen *template*. Aangezien het biometrische kenmerk niet altijd exact overeen zal komen met het *template*, wordt een zekere afwijking toegestaan. Deze afwijking mag niet te groot zijn, omdat het dan geen betrouwbaar herkenningsmiddel meer is, maar ook niet te klein, omdat anders gebruikers ten onrechte kunnen worden afgewezen.
Biometrische herkenningsmethoden worden veelal gebruikt in combinatie met een *smart card*. Dit gebeurt niet alleen uit doelmatigheid (de controle kan sneller plaatsvinden als geen contact hoeft te worden gezocht met een centrale databank), maar is ook uit privacyoverwegingen belangrijk (bij decentrale opslag is het risico van koppeling van persoonsgegevens en bestanden kleiner). Ook kan de combinatie van bezit (de *smart card*) en het persoonskenmerk de betrouwbaarheid en veiligheid van de herkenningsmethode vergroten. De kans dat een ongeautoriseerde gebruiker én de *smart card* heeft én een correct biometrisch kenmerk heeft dan wel weet te reproduceren is namelijk kleiner dan dat slechts een van beide vereist is voor herkenning of autorisatie.

Vanuit de wens om reisdocumenten beter te beveiligen tegen vooral *look-alike*-fraude, heeft het kabinet onderzoek verricht naar de mogelijkheden van het gebruik van biometrische kenmerken in het paspoort en de betrouwbaarheid van biometrische technieken. Daarnaast is een overweging voor de toevoeging van biometrische kenmerken aan reisdocumenten dat hiermee nieuwe mogelijkheden worden geschapen voor geautomatiseerde identiteitsvaststelling en een efficiëntere afhandeling van de grenscontrole. Het accent ligt bij de voorziene toepassing van biometrie in reisdocumenten met name op gezichtsherkennings-, vingerafdruk- en irisscantechnologie.[43] De overheid beoogt biometrie in combinatie met een smartcard en PKI-technologie toe te passen.[44]

Organisatorische context
Het proces van ontwikkeling van *templates* zal met waarborgen moeten worden omkleed en beveiligd. Ook dienen de *templates* dusdanig te worden opgeslagen dat eventuele manipulatie zo goed als uitgesloten is. Daartoe kan gebruik worden gemaakt van media die slechts eenmaal beschreven kunnen worden en niet te manipuleren zijn.

De opgeslagen *templates* moeten vervolgens toegankelijk zijn voor geautoriseerden teneinde een vergelijking met voor verificatie gemaakte *templates* mogelijk en het proces van herkenning uitvoerbaar te maken. Naast opslag op *smart cards* (zie boven), kunnen templates ook in een centrale databank worden opgeslagen en online toegankelijk zijn voor geautoriseerden. Dat betekent dat er autorisatie- en beveiligingsprocedures dienen te worden opgesteld om adequate beveiliging van de gegevens te waarborgen en ongeautoriseerde toegang uit te sluiten. De opslag kan ook gedistribueerd over verschillende databanken worden opgeslagen, zodat bij corruptie van één databank de overige databanken als reservekopie fungeren en beschikbaarheid garanderen. Door middel van *remote copy*-technieken kan ervoor worden gezorgd dat dezelfde *templates* in verschillende databanken wordt opgeslagen. Voorts kan een TTP worden ingeschakeld om betrouwbare en veilige opslag van en toegang tot *templates* te realiseren. Tevens kan in het licht van beveiliging worden gedacht aan certificering van opslag- en toegangssystemen.

[43] Zie Jaarplan 2003 van het agentschap Basisadministratie Persoonsgegevens en Reisdocumenten, Minister van Binnelandse Zaken en Koninkrijkrelaties, p. 23-24, <http://www.bprbzk.nl/downloads/jaarplan%202003.pdf>.
[44] *Kamerstukken II* 2001/02, 28 342 (R 1719), nr. 3, p. 2.

In het kader van het bovengenoemde idee reisdocumenten te beveiligen met biometrie, zijn wijzigingen van de Paspoortwet voorgesteld.[45] Hierbij wordt voorzien in een door privacyoverwegingen ingegeven beveiliging van gegevens omtrent biometrische kenmerken van de houder van een reisdocument. Het wetsvoorstel vereist een zodanige verwerking van deze gegevens in elektronisch vorm dat daaruit geen fysieke of persoonlijke kenmerken kunnen worden opgemaakt. Het is verder de bedoeling om de gegevens op de chip op het reisdocument op te slaan en bij verificatie niet op te nemen in bestanden van de instelling die de verificatie uitvoert om verspreiding ervan te voorkomen. Wel wordt het gegeven toegevoegd aan de andere persoonsgegevens die reeds zijn opgeslagen in de reisdocumentenadministratie. Deze administratie mag slechts worden geraadpleegd in geval van vermissing van reisdocumenten en andere bijzondere omstandigheden in het gebruik van reisdocumenten waarbij verificatie van de identiteit van de betrokkene noodzakelijk is. De raadpleging van de administratie is gebonden aan regels in verschillende paspoortuitvoeringsregelingen. Het wetsvoorstel, dat eind 2003 in het parlement in behandeling is, voorziet echter in een kader specifiek voor de verstrekking van biometrische gegevens.[46] Verstrekking van de gegevens is voorbehouden aan met de uitvoering van de Paspoortwet belaste autoriteiten en aan met opsporing belaste ambtenaren bij vermoeden van fraude met of misbruik van het reisdocument (ontwerpartikel 3 lid 11). Ook kunnen slechts aan de hand van naam of het nummer van het reisdocument van betrokkene en dus niet willekeurig gegevens worden verstrekt uit de administratie met het oog op verificatie van de identiteit van betrokkene (ontwerpartikel 3 lid 14). Bij ministeriële regeling kunnen nadere organisatorische voorschriften worden gegeven (ontwerpartikel 3 lid 13).

Juridische context

Bij de juridische context moet onderscheid worden gemaakt tussen juridische aspecten rondom het gebruik van biometrie als zodanig en de juridische status van biometrie als elektronische handtekening.

In het eerste geval kan een verplichting tot het gebruik van biometrie een wettelijke basis vereisen, omdat de toepassing een inbreuk op het grondrecht van lichamelijke integriteit (artikel 11 Gw) of van eerbiediging van de persoonlijke levenssfeer (artikel 10 Gw) kan vormen. Hierbij kan onder meer meespelen of er aan burgers andere opties openstaan dan alleen herkenning door biometrie. Indien het gebruik van biometrie op basis van vrijwilligheid gebeurt, zal men kunnen aannemen dat de persoon in kwestie instemt, en is er geen sprake van een inbreuk op een grondrecht. Dit kan overigens weer anders liggen wanneer sprake is van gevoelige gegevens, zoals het gebruik van gegevens omtrent iemands ras. Hiervan kan sprake zijn bij biometrische herkenning. De Wet bescherming persoonsgegevens (Wbp) stelt zwaardere eisen aan het gebruik van gevoelige persoonsgegevens bij biometrische herkenning. In beginsel geldt een verbod (artikel 16), maar een uitzondering kan onder meer worden gemaakt met het oog op identificatie van een persoon voor zover dit voor dit doel onvermijdelijk is (artikel 18). De voor het biometrische herkenningsproces gebruikte *templates* kunnen voorts ook meer in het algemeen persoonsgegevens in de zin van de Wbp zijn, zodat de verplichting om te zorgen voor een passend beveiligingsniveau (artikel 13 Wbp) van toepassing is.

Biometrie kan evenals de digitale handtekening worden toegepast als elektronische handtekening. Het kan handtekeningfuncties als het verifiëren van iemands identiteit, het authenticeren van verklaringen en autoriseren van handelingen vervullen. Op grond van richtlijn 1999/93/EG inzake elektronische handtekeningen mogen biometrische herkenningsmethoden geen juridische geldigheid worden ontzegd. In de regel zal bij biometrische herkenningsmethoden geen sprake zijn van een door een CA uitgegeven gekwalificeerd digitaal certificaat, zodat geen sprake zal zijn van een volledige gelijkstelling met de handmatige handtekening op grond van artikel 5 lid 1 van deze richtlijn.

[45] *Kamerstukken II* 2001/02, 28 342 (R 1719), nrs. 1-2.
[46] Zie alles *Kamerstukken II* 2001/02, 28 342 (R 1719), nr. 3, p. 3-4.

Het eerder genoemde in april 2002 bij het parlement ingediende wetsvoorstel tot wijziging van de Paspoortwet in verband met de toepassing van biometrie in reisdocumenten[47] bepaalt dat naast de foto en handtekening tevens biometrische kenmerken aan het paspoort zullen kunnen worden toegevoegd ter verificatie of de houder dezelfde persoon is als degene aan wie het paspoort is verstrekt (ontwerpartikel 3 lid 8). In welke reisdocumenten biometrische kenmerken kunnen worden opgenomen en welke biometrische kenmerken het betreft, zal nader kunnen worden bepaald bij algemene maatregel van rijksbestuur (ontwerpartikel 3 lid 9). Met de juridische inbedding van de toepassing van biometrie in reisdocumenten wordt mede toegegeven aan internationale druk omtrent het onderwerp, aangezien de *International Civil Aviation Organisation* (ICAO), die richtlijnen betreffende de acceptatie van reisdocumenten vaststelt, naar verwachting met een richtlijn omtrent biometrie in reisdocumenten komt. De richtlijnen hebben weliswaar geen dwingend karakter, maar worden door de Europese Unie over het algemeen in resoluties over in de Europese Unie gebruikte reisdocumenten overgenomen. Voor de acceptatie van Nederlandse reisdocumenten in het buitenland wordt het dan ook van belang geacht om met (te verwachten) internationale ontwikkelingen in dit verband in de pas te lopen.[48]

6.3.3. Primair organisatorische maatregelen

6.3.3.1. Interne maatregelen

Naast de organisatorische maatregelen die de primair technische maatregelen flankeren, zoals de certificatiedienst bij digitale handtekeningen, zijn er ook maatregelen waarbij de organisatorische component meer voorop staat en waarbij de techniek deze organisatorische maatregelen ondersteunt. De meeste van deze organisatorische maatregelen zijn intern gericht en hebben te maken met de wijze waarop de toegang tot informatie en tot computers wordt beschermd.
De bekendste vorm van interne organisatorische maatregelen is toegangscontrole. Deze bestaat veelal uit een fysieke en een elektronische component. Bij fysieke toegangscontrole moet men denken aan maatregelen die de toegang tot een gebouw of een deel daarvan beperken, zoals een receptie en/of een pasjessysteem. Toegangspassen kunnen op hun beurt verder worden beveiligd met bijvoorbeeld biometrie. Fysieke toegangscontrole kan ook bestaan uit tradionele maatregelen als het opbergen van reservebestanden in een kluis, of het plaatsen van een *stand-alone* computer in een afgesloten ruimte waar slechts een deel van het personeel toegang toe heeft.
Elektronische toegangscontrole bestaat uit maatregelen die de toegang tot een computernetwerk beschermen, zoals een inlogprocedure met gebruikersnaam en wachtwoord, maar ook uit beperkingen in het gebruik van het netwerk. Bepaalde delen van een netwerk met gevoelige informatie of kritische functies kunnen worden afgeschermd tegen algemene toegang, zodat alleen degenen die vanuit hun functie toegang moeten hebben tot deze delen daadwerkelijk hierbij kunnen. De toegangscontrole bij computernetwerken die verbonden zijn met de buitenwereld zal ook gericht moeten zijn op beveiliging tegen externe aanvallen. De bekendste vorm van externe beveiliging van een computernetwerk is een brandmuur (*firewall*), een systeem dat controleert welke gegevenspakketten het interne netwerk in of uit mogen.
Een tweede interne organisatorische maatregel betreft viruscontrole, tegenwoordig een standaardprocedure bij computers die zijn verbonden met een netwerk. In bepaalde gevallen is het echter wenselijk om aanvullende bescherming tegen virussen te bieden: bij bijzonder gevoelige gegevens of systemen kan het wenselijk zijn om elke mogelijkheid van virusindringing uit te sluiten door deze gegevens of systemen uit het netwerk te halen en op zelfstandige computers te plaatsen, waarop alleen schijfjes kunnen worden gebruikt die eerst op een proefcomputer zijn getoetst op virussen.

[47] *Kamerstukken II* 2001/02, 28 342 (R 1719), nrs. 1-2.
[48] Zie alles *Kamerstukken II* 2001/02, 28 342 (R 1719), nr. 3, p. 2-3.

Voor een goed functioneren van dergelijke maatregelen is meer vereist dan alleen het installeren van een technisch middel en het instrueren van het personeel. Ten eerste is continuïteit belangrijk: na verloop van tijd slijten procedures als zij niet periodiek worden opgefrist. Toezicht op naleving van organisatorische maatregelen is daarom een belangrijk middel om de beveiliging op peil te houden. Een hulpmiddel is voorts adequate logprocedures, zodat bij incidenten kan worden nagegaan wat er wanneer is gebeurd, maar ook om routinematig te controleren of procedures worden nageleefd. Misschien wel het belangrijkste hulpmiddel in dit opzicht is educatie: bewustwording van kwetsbaarheid en van het belang van naleving van beveiligingsprocedures komt niet vanzelf. De werknemers zullen door middel van bewustwordingsmaatregelen moeten worden doordrongen van de noodzaak zich te houden aan procedures als wachtwoordbeheer en viruscontrole.

6.3.2. Externe maatregelen

Een veelgenoemde externe maatregel voor informatiebeveiliging is het inschakelen van een derde partij. *Trusted Third Parties* (TTP's) kunnen worden ingezet om de betrouwbaarheid van het informatie- en communicatieverkeer te vergroten. De TTP kan verschillende verschijningsvormen aannemen en diverse functionaliteiten uitoefenen. Meestal staat daarbij op een of andere manier het waarborgen van de integriteit van informatie centraal, maar een TTP kan ook worden gebruikt om de beschikbaarheid of vertrouwelijkheid van gegevens te waarborgen. Bij de digitale handtekeningen (par. 6.2.2) is reeds ingegaan op de TTP die publieke sleutels voor ondertekening certificeert, hetgeen in de praktijk vooralsnog de belangrijkse functie van een TTP is. Maar een TTP ook kan ook tijdstempeldiensten (*time-stamping*) aanbieden, waarbij wordt gegarandeerd dat gegevens op een bepaalde datum en tijd zijn aangemaakt of verstuurd, of bewijs- en bewaardiensten, zoals het bewaren van publieke sleutels en hun certificaten, ondertekende digitale documenten en reservekopieën.

Bij externe maatregelen moet men ook denken aan meer algemene, preventieve maatregelen, die niet zozeer gericht zijn op één specifieke organisatie als wel op de informatiebeveiliging in een sector of geografisch gebied. Er zijn kenniscentra die zich richten op vergaren en verspreiden van kennis over incidenten en beveiligingsmaatregelen; in Nederland is bij ECP.NL bijvoorbeeld het eerder genoemde programma KWINT ondergebracht, dat werkt aan oplossingen op het gebied van continuïteit van Internet in Nederland, verstikkingsaanvallen (*denial-of-service*aanvallen), virussen, hacking, integriteit van informatie (inclusief authenticatie), transparantie van Internet, misbruik door eigen personeel en exclusiviteit van informatie (waaronder creditcardgegevens).[49]
Een veelvoorkomend fenomeen is een Computer Emergency Response Team (CERT), dat bij een dreiging prompt kan ingrijpen, bijvoorbeeld door een viruswaarschuwing te doen uitgaan zodra een nieuw en potentieel grootschalig virus is gesignaleerd; zo kan als een virus zich in Australië heeft geopenbaard bij het begin van een werkdag, een prompte waarschuwing van Europese en Amerikaanse bedrijven die dan nog niet zijn begonnen voorkomen dat het virus zich wereldwijd grootschalig verspreidt.
In Nederland is sinds juni 2002 het Computer Emergency Response Team van de Nederlandse overheid (GOVCERT.NL) officieel actief op het gebied van ICT-veiligheid. GOVCERT.NL richt zich naast overheidsorganisaties ook op de Nederlandse burger en het kleinbedrijf. Het biedt ondersteuning op het gebied van preventie en afhandeling van ICT-gerelateerde veiligheidsincidenten, zoals computervirussen, hacking en fouten in applicaties en hardware. Voorts fungeert het als centraal meld- en coördinatiepunt voor veiligheidsincidenten en wordt door middel van kennisuitwisseling bijgedragen aan verhoging van het kennisniveau omtrent veiligheidsincidenten en standaardisatie van werkwijzen.[50]

[49] Zie <http://www.ecp.nl/dossieritem.php?dossier_id=6> en <http://www.kwint.org>.
[50] Zie alles <http://www.govcert.nl>.

In februari 2003 heeft GOVCERT.NL een waarschuwingsdienst in het leven geroepen, die burgers en kleine bedrijven waarschuwt tegen dreigende beveiligingsincidenten, zoals nieuwe virussen en hackpogingen. De Waarschuwingsdient publiceert hierover op een weblocatie, maar men kan zich ook abonneren op een mailinglijst of sms-dienst die de waarschuwingen uitstuurt.[51]

7. Afsluiting

We hebben gezien dat de penetratie van ICT in de vezels van het alledaagse functioneren van de samenleving en de vervlechting van ICT-netwerken met andere netwerken en infrastructuren verregaand is. In het DNA van de westerse samenleving zit ICT. Daardoor is diezelfde samenleving uiterst kwetsbaar geworden, zeker daar waar het knooppunten en zenuwcentra betreft. Het gaat daarbij om risico's die de stabiliteit en de continuïteit van de samenleving kunnen bedreigen – risico's die daarmee een van de kerntaken van de overheid raken. Tegelijkertijd leren Castells en Beck ons dat de wederzijdse afhankelijkheid in de netwerksamenleving zo complex is en dat de potpourri van effecten zo gevarieerd, zo onoverzichtelijk kan zijn en zich kan manifesteren op dusdanig uiteenlopende schaalniveaus, dat het haast ondoenlijk is om de zorg voor deze kwetsbaarheden alleen maar voor rekening van de overheid te laten komen. Vandaar dat het van belang om de aandacht en zorg voor kwetsbaarheden in de netwerksamenleving vorm en inhoud te geven op grond van drie sturingsmodellen (zie Bekkers e.a., 2002), waarbij het niet alleen de staat is die door middel van wet- en regelgeving en door middel van toezicht en handhaving bepaalde veiligheidsrisico's ('command and control') beheersbaar tracht te maken – voorzover dit mogelijk is. Het open en dynamische karakter van de netwerksamenleving vereist dat we de zorg voor deze kwetsbaarheden ook tot een verantwoordelijkheid maken van andere partijen. Ook private partijen hebben daarin een eigen verantwoordelijkheid, waarbij door middel van vormen van zelfregulering getracht een eigen risicobeleid te voeren. Daarbij kunnen we denken aan de ontwikkeling van kwaliteitsstelsels en certificeringstelsels, maar ook aan bewustwordingsbeleid en scholing. Waar nodig kan de overheid het ontstaan van deze op veiligheid georiënteerde kwaliteitsstelsels faciliteren en stimuleren, dan wel hiervoor wettelijke kaders ontwikkelen (zelfregulering binnen kaders). Ten slotte is het ook van belang om burgers en maatschappelijke organisaties een actieve rol te geven in het agenderen van deze kwetsbaarheden, alsmede hun een positie te geven als mede-toezichthouder. Niet voor niets pleit Beck voor een verdere vermaatschappelijking van het debat over risico's, buiten de gebaande paden van de veiligheidsdeskundigen om. Het via het internet toegang geven tot bepaalde informatiebronnen over mogelijke risico's is daarbij een eerste stap (zie ook het hoofdstuk over toezicht van Bekkers en Homburg) Met deze informatie in de hand kunnen burgers vervolgens bepaalde risico's aankaarten en overheden vragen hoe zij met deze risico's omgaan.

Aan de andere kant moet ook worden benadrukt dat, hoewel private partijen een belangrijke rol hebben bij het beheersbaar maken en houden van de risico's, het onaanvaardbaar is als de verantwoordelijkheid geheel bij de private sector zou worden neergelegd. De kwetsbaarheid van de netwerksamenleving is van dusdanig fundamenteel belang dat de overheid een belangrijke rol moet vervullen bij de beveiliging van de ICT-infrastructuren. Proactief optreden door stimuleren van bewustwording, beveiligingsbeleid en beveiligingsmaatregelen, het scheppen van de juiste juridische en organisatorische randvoorwaarden, en een voortdurende alertheid op nieuwe ontwikkelingen en bedreigingen zijn vereist. Daarbij past een meer actieve houding dan uit de nota KWINT blijkt: beveiliging tegen ICT-kwetsbaarheid dient meer te zijn dan een verzameling losse actiepunten van uiteenlopende aard die her en der onderweg zijn; een visie op de toekomst van de kwetsbare netwerksamenleving en een daaruit voortvloeiend samenhangend pakket van maatregelen door publieke en private partijen zijn dringend gewenst.

Kortom, de kwetsbaarheden in de netwerksamenleving vragen niet om de keuze voor één sturingsmodel, maar om een combinatie van meerdere modellen, die bovendien recht doen aan

[51] Zie <http://www.waarschuwingsdienst.nl/> en <http://www.govcert.nl/render.html?it=159>.

de grote mate van variëteit van risico's. Want ook hier geldt, indachtig Linus' law: "given enough eyes, all bugs are shallow" (Bekkers, 2000): hoe meer ogen kijken, hoe eerder risico's kunnen worden opgespoord. Een beleid dat recht wil doen aan de kwetsbaarheden in de netwerksamenleving vraagt om het organiseren van meerdere, deels concurrerende, deels overlappende en deels complementaire perspectieven.

Literatuur

Aalberts & Van der Hof 2000
Babette Aalberts, Simone van der Hof, *Digital Signature Blindness*, ITeR-deel 32, Deventer: Kluwer 2000.

Beck 1994
U. Beck, 'The reinvention of politics, Towards a theory of reflexive modernization', in: Beck, U, A. Giddens & S. Lash, *Reflexive modernization*, Cambridge: Polity Press 1994, p. 1-55.

Beck 1999
U. Beck, *World risk society*, Cambridge: Polity Press 1999.

Bekkers 2000
V.J.J.M. Bekkers, *Voorbij de virtuele organisatie*, Den Haag: Elsevier 2000.

Bekkers e.a. 2002
V.J.J.M. Bekkers, M. Thaens, V.M.F. Homburg, J. Ragetlie & M. de Rooij, *De keerzijde van verbonden netwerken: de relatie overheid-burger in de netwerksamenleving*, Delft: Eburon 2002.

Castells 1996
M. Castells, *The rise of the network society*, Malden/Oxford: Blackwell Publ. 1996.

Code voor Informatiebeveiliging 2000
Nederlands Normalisatie-instituut, Code voor Informatiebeveiliging, Delft 2000.

Douglas & Wildavsky 1982
M. Douglas & A. Wildavsky, *Risk and culture*, Berkely: UCP 1982.

Enquêtecommissie 1994
Enquêtecommissie opsporingsmethoden, *Inzake opsporing*, Den Haag: Sdu 1996.

Garfinkel 1997
Simson Garfinkel, *Web Security & Commerce*, Cambridge etc.: O'Reilly 1997.

Huigen & Bekkers 1994
J. Huigen & V. Bekkers, 'Wegwijs op de digitale snelweg: over belangen en impasses', in: V.J.J.M. Bekkers, *Wegwijs op de digitale snelweg*, Amsterdam: Cramwinckel 1994, p. 13-28.

Himanen 2001
Pekka Himanen, *The Hacker Ethic, and the Spirit of the Information Age*, New York: Random House 2001.

Van der Hof 2003
Simone van der Hof, *Digital Signature Law Survey*, 2003 <http://rechten.uvt.nl/simone/ds-lawsu.htm>.

Koops & De Jong 1998
Bert-Jaap Koops & Huub de Jong, 'De risico's van data recovery voor overheid en gebruikers', *Computerrecht* 1998/5, p. 222-227.

Koops & Van der Wees 1998
Bert-Jaap Koops, Leo van der Wees, 'Woordenlijst dossier Trusted Third Parties', Computerrecht 1998/5, p. 233-234.

Koops 2002
Bert-Jaap Koops, *Crypto Law Survey*, versie 21.0, oktober 2002, <http://rechten.uvt.nl/koops/cryptolaw/>.

Kolkman & Van Kralingen 1998

Pascal Kolkman & Robert van Kralingen, *Verschuivend vertrouwen. Methoden voor het waarborgen van betrouwbaarheid in het elektronisch rechtsverkeer*, ITeR-deel 12, Deventer: Kluwer 1998.

Kristof & WuDunn 1994

Nicholas D. Kristof & Sheryl WuDunn, *China Wakes*, London: Nicholas Brealey Publishing 1994.

Van Kralingen, Prins & Grijpink 1997

Robert van Kralingen, Corien Prins & Jan Grijpink, *Het lichaam als sleutel*, ITeR-deel 8, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997, p. 3-66.

Menezes, Van Oorschot & Vanstone 2001

Alfred J. Menezes, Paul C. van Oorschot & Scott A. Vanstone, *Handbook of Applied Cryptography*, 5th printing, CRC Press 2001 (de eerste druk uit 1996 is beschikbaar op http://www.cacr.math.uwaterloo.ca/hac/>).

Negroponte 1995

N. Negroponte, *Being Digital*, New York: Knopf 1995.

Schneier 1996

Bruce Schneier, *Applied Cryptography. Protocols, Algorithms, and Source Code in C*, 2nd edition, New York etc.: John Wiley & Sons 1996.